

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

ROBERTO CHAPMAN, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

COLUMBIA BANKING SYSTEMS, INC.,
d/b/a UMPQUA BANK,

Defendant.

No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Roberto Chapman (“Plaintiff”), individually and on behalf of all other similarly situated individuals (the “Class Members,” as defined below), by and through her counsel, files this Class Action Complaint against Columbia Banking Systems, Inc., d/b/a Umpqua Bank (“Umpqua” or “Defendant”) and alleges the following based on personal knowledge of facts pertaining to herself and on information and belief based on the investigation of counsel as to all other matters.

INTRODUCTION

1. During an undisclosed time frame, an unknown actor gained access to Umpqua Bank’s files that were saved on its MOVEit server. As a result, Plaintiff and the Class Members

1 (as further defined below) have had their personal identifiable information (“PII”)¹ exposed (the
2 “Data Breach”). It is believed that the well-known Russian cybergang, CL0P (“Clop”) is the source
3 of the attack.²

4 2. In carrying out its business, Defendant obtains, collects, uses, and derives a benefit
5 from the PII of Plaintiff and Class Members. As such, Defendant assumed the legal and equitable
6 duties to those individuals to protect and safeguard that information from unauthorized access and
7 intrusion.

8 3. On May 31, 2023, Umpqua knew or should have known of a critical security
9 vulnerability impacting the MOVEit Secure File Transfer server that it used. Despite this,
10 Defendant fails to take any steps to mitigate the vulnerability or protect Plaintiff and the Class
11 Members’ PII, failed to investigate the vulnerability and any potential attack into their system, and
12 failed to inform Plaintiff and the Class Members that their PII was at significant risk of being
13 stolen.

14 4. On or around June 21, 2023, Defendant claims they became aware that its MOVEit
15 system had been breached.

16 5. According to Defendant, the PII exposed in the Data Breach includes Social
17 Security Numbers.

18 6. Around August of 2023, Defendant began notifying Plaintiff and Class Members
19 of the Data Breach.

20
21
22
23
24
25
26 ¹ Personal identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

² <https://securityintelligence.com/news/the-moveit-breach-impact-and-fallout-how-can-you-respond/>.

1 7. Due to Defendant's negligence, cybercriminals obtained everything they need to
2 commit identity theft and wreak havoc on the financial and personal lives of thousands of
3 individuals.

4 8. This class action seeks to redress Defendant's unlawful, willful and wanton failure
5 to protect the personal identifiable information of approximately 429,252 individuals³ that was
6 exposed in a major data breach of Defendant's files saved on the MOVEit server in violation of its
7 legal obligations.

8 9. For the rest of their lives, Plaintiff and the Class Members will have to deal with
9 the danger of identity thieves possessing and misusing their Personal Information. Plaintiff and
10 Class Members will have to spend time responding to the Breach and are at an immediate,
11 imminent, and heightened risk of all manners of identity theft as a direct and proximate result of
12 the Data Breach. Plaintiff and Class Members have incurred and/or will continue to incur damages
13 in the form of, among other things, identity theft, attempted identity theft, lost time and expenses
14 mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their Personal
15 Information, loss of privacy, and/or additional damages as described below.

16 10. Defendant betrayed the trust of Plaintiff and the other Class Members by failing to
17 properly safeguard and protect their personal identifiable information and thereby enabling
18 cybercriminals to steal such valuable and sensitive information.

19 11. At this time, there exist many Class Members who are totally unaware their PII has
20 been compromised, and that they are at significant risk of identity theft and various other forms of
21 personal, social, and financial harm.
22
23
24
25
26

³ See <https://apps.web.maine.gov/online/aeviewer/ME/40/7589df9f-75b6-417f-afa0-68eeec2e7de9.shtml>.

24. Plaintiff and Class Members relied on this sophisticated Defendant to keep their Personal Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their Personal Information.

25. Defendant used the file transfer software MOVEit to move, store, and share files containing the Plaintiff and Class Members' PII.

26. Defendant had a duty to adopt reasonable measures to protect the Personal Information of Plaintiff and the Class Members from involuntary disclosure to third parties, including ensuring that all software used to move, store, and/or share PII was secure.

Known Vulnerability in MOVEit

27. Progress Software Corporation ("PSC") owns and operates a file transfer management program known as MOVEit. PSC claims that the program provides secure collaboration and automated file transfers of sensitive data and advanced workflow automation capabilities without the need for scripting.⁴

28. However, the MOVEit software had a critical zero-day flaw.⁵ This critical zero-day flaw led to a wave of cyber-attacks against organizations who collected the sensitive PII/PHI.⁶ Multiple organizations have now confirmed data breaches.⁷

29. On or around May 27, 2023, Cl0p began its hacking campaign against the MOVEit software, exploiting the zero-day vulnerability.⁸ Though, some reports indicate that Cl0p began

⁴ <https://www.progress.com/moveit>.

⁵ "A zero-day vulnerability is a vulnerability in a system or device that has been disclosed but is not yet patched. An exploit that attacks a zero-day vulnerability is called a zero-day exploit." See <https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability>.

⁶ See <https://www.techtarget.com/searchsecurity/news/366539672/MoveIt-Transfer-flaw-leads-to-wave-of-data-breach-disclosures>

⁷ *Id.*

⁸ <https://www.upguard.com/blog/the-moveit-0-day>.

exploiting and access the server months before then.⁹

30. On or around May 28, 2023, PSC received notice of the breach.

31. On or around May 31, 2023, PSC posted a notice on its website confirming the vulnerability in MOVEit and warning users that the vulnerability could result in an unauthorized party gaining access to their computer networks.¹⁰

32. By June 2, 2023, PSC had released a patch for the vulnerability.¹¹

33. Throughout June of 2023, PSC again publicly disclosed that its MOVEit Transfer tool had been compromised and continued releasing patching and mitigating information and efforts to avoid data breaches.

Defendant's Data Breach

34. On an undisclosed date, information intentionally withheld from the public, due to Defendant's failure to maintain an adequate security system, an unknown hacker gained access to the Plaintiff and the Class's PII.

35. Defendant utilized the services provided by its vendors with complete disregard for its vendors' data security, infrastructure, procedures, and protocols.

36. Defendant knew of its duties to Plaintiff and the Class Members, and the risks associated with failing to protect the PII entrusted to it. Defendant knew that if it did not select a vendor with adequate security that Plaintiff's and the Class's PII would be unlawfully exposed.

37. Upon information and belief, Defendant failed to properly inquire about MOVEit's data security before entrusting it with Plaintiff's and the Class's PII and failed to monitor and oversee MOVEit's data security throughout their relationship. Had Defendant properly inquired

⁹ <https://www.bleepingcomputer.com/news/security/clop-ransomware-likely-testing-moveit-zero-day-since-2021/>.

¹⁰ <https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023>.

¹¹ *Id.*

1 about MOVEits's data security, overseen MOVE's data security, and monitored MOVEit's data
2 security, Plaintiff's and the Class's PII would have never been exposed in the Data Breach.

3 38. Defendant had notice of the critical vulnerability and likely chance of a data breach
4 as early as May 31, 2023. Yet, Defendant negligently delayed in responding to the breach and
5 informing Plaintiff and the Class of the breach.
6

7 39. Defendant claim that it received notice of the Data Breach on June 21, 2023.

8 40. On or around August 2023, Defendant began sending Plaintiff and Class Members
9 undated notices of the Data Breach ("Notice of the Data Breach").¹²

10 41. Defendant admitted in the Notice of the Data Breach that an unauthorized actor
11 accessed sensitive personal information about Plaintiff and Class Members.

12 42. The details of the root cause of the Data Breach, the vulnerabilities exploited, and
13 the remedial measures undertaken to ensure a breach does not occur again have not been shared
14 with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their
15 information remains protected.
16

17 43. The unencrypted PII of Plaintiff and Class Members may end up for sale on the
18 dark web, or simply fall into the hands of companies that will use the detailed PII for targeted
19 marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can
20 easily access the PII of Plaintiff and Class Members.

21 44. Defendant was negligent and did not use or implement reasonable security
22 procedures, oversight and practices appropriate to the nature of the sensitive, unencrypted
23 information it was maintaining for Plaintiff and Class Members, causing the exposure of PII for
24 Plaintiff and Class Members.
25

26

¹² See **Exhibit 1**

1 45. Because Defendant had a duty to protect Plaintiff's and Class Members' PII,
2 Defendant should have known through readily available and accessible information about potential
3 threats for the unauthorized exfiltration and misuse of such information.

4 ***The Data Breach was Foreseeable***

5 46. Preceding the Data Breach, Defendant knew or should have known that
6 Defendant's MOVEit server was a target for cybersecurity attacks because warnings were readily
7 available and accessible via the internet.

8
9 47. Preceding the Data Breach, Defendant failed to take reasonable and necessary steps
10 to ensure the its MOVEit system was secure.

11 48. Preceding the Data Breach, Defendant received notice of the critical vulnerability
12 in MOVEit's system. Despite this, Defendant still failed to take steps to ensure that Plaintiff and
13 Class Members' Personal Information was secure.

14 49. In October 2019, the Federal Bureau of Investigation published online an article
15 titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that,
16 among other things, warned that "[a]lthough state and local governments have been particularly
17 visible targets for ransomware attacks, ransomware actors have also targeted health care
18 organizations, industrial companies, and the transportation sector."¹³

19
20 50. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in
21 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive
22 in their pursuit of big companies. They breach networks, use specialized tools to maximize
23 damage, leak corporate information on dark web portals, and even tip journalists to generate
24

25
26 ¹³ FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), available at <https://www.ic3.gov/Media/Y2019/PSA191002> (last visited Aug. 17, 2023).

negative news for companies as revenge against those who refuse to pay.”¹⁴

51. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a “Ransomware Guide” advising that “[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion.”¹⁵

52. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that: (i) cybercriminals were targeting big companies such as Defendant and Defendant’s clients, (ii) cybercriminals were ferociously aggressive in their pursuit of companies in possession of significant sensitive information such as Defendant and Defendant’s clients, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals’ tactics included threatening to release stolen data.

53. Considering the information readily available and accessible on the internet before the Data Breach and Defendant’s involvement in data breach litigation, Defendant, having elected to store the unencrypted PII of Plaintiff and Class Members with a third-party without first ensuring that the third party’s system was secure, Defendant had reason to know that Plaintiff and the Class Members PII was at risk for being shared with unknown and unauthorized persons.

54. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff’s and Class Members’ PII could be accessed, exfiltrated, and published as the result of a cyberattack.

¹⁴ 5 ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), available at <https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/> (last visited Aug. 17, 2023).

¹⁵ U.S. CISA, Ransomware Guide – September 2020, available at https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last visited Aug. 17, 2023).

55. Prior to the Data Breach, Defendant knew or should have known that it should have confirmed the information it obtained was encrypted within the PII to protect against their publication and misuse in the event of a cyberattack.

56. Prior to the Data Breach, Defendant knew or should have known that it should have confirmed with PSC that MOVEit's systems were secure and capable of protecting Plaintiff and the Class Members PII.

57. Since the breach, Defendant continues to store patient information, including Plaintiff's and Class Members' PII and has failed to give adequate assurances that it has enhanced its security practices sufficiently to avoid another breach of its servers in the future. It has also failed to assure Plaintiff and the Class Members that it will or has terminated its use of MOVEit.

Defendant's Response to the Data Breach is Inadequate

58. Defendant was negligent and failed to inform Plaintiff and the Class Members of the Data Breach in time for them to protect themselves from identity theft.

59. Defendant admitted that it learned of the data breach as early as June 21, 2023. Yet, Defendant did not start notifying affected individuals until almost a year later on or around mid-August 2023.

60. During these intervals, the cybercriminals have had the opportunity to exploit the Plaintiff and the Class Member's Personal Information while Defendant was secretly investigating the Data Breach.

Plaintiff's Experiences

61. Plaintiff received banking services from Umpqua Bank or one of its affiliates. In exchange, Umpqua required Plaintiff's PII.

62. Defendant acquired, collected, and stored Plaintiff's PII and transferred it in the MOVEit Software.

63. Defendant was obligated by law, regulations, and guidelines to protect Plaintiff's and the Class's PII and Defendant was required to ensure both it and its vendors maintained adequate data security, infrastructure, procedures, and protocols for Plaintiff's and the Class's PII.

64. Defendant was in possession of Plaintiff's PII before, during, and after the Data Breach.

65. Plaintiff received Defendant's Notice of Data Breach in August of 2023. The Notice stated that Plaintiff's PII was impacted by the Data Breach, including his name and Social Security number.

66. As a result of the Data Breach, Plaintiff's sensitive information may have been accessed and/or acquired by an unauthorized actor, including his name, Social Security number. Defendant has not yet provided definitive findings for Plaintiff to know. The confidentiality of Plaintiff's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff will have to worry about when and how his sensitive information may be shared or used to his detriment.

67. As a result of the Data Breach, Plaintiff has seen a significant increase in spam calls including calls regarding loans for which he has not applied. Plaintiff has also received text messages from loan officers regarding loans for which he never applied.

68. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

69. Additionally, Plaintiff is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

70. Plaintiff stores any documents containing his sensitive PII in safe and secure

1 locations or destroys the documents. Moreover, he diligently chooses unique usernames and
2 passwords for her various online accounts.

3 71. As a direct and traceable result of the Data Breach, Plaintiff suffered actual
4 damages such as: (i) lost time related to monitoring her accounts for fraudulent activity; (ii) loss
5 of privacy due to his PII being exposed to cybercriminals; (iii) loss of the benefit of the bargain
6 because Defendant did not adequately protect his PII; (iv) severe emotional distress because
7 identity thieves now possess his PII; (v) exposure to increased and imminent risk of fraud and
8 identity theft now that his PII has been exposed; (vi) the loss in value of his PII due to his PII being
9 in the hands of cybercriminals who can use it at their leisure; (vii) actual misuse of his PII; and
10 (viii) other economic and non-economic harm.

12 72. Plaintiff has experienced actual misuse of his PII. After the breach, Plaintiff
13 experienced a significant increase in spam calls and text messages and has also experienced
14 fraudulent accounts opened in his name.

16 73. Plaintiff has suffered imminent and impending injury arising from the substantially
17 increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands
18 of unauthorized third parties and possibly criminals.

19 74. Plaintiff has a continuing interest in ensuring that his PII, which, upon information
20 and belief, remains backed up in Defendant's possession, is protected and safeguarded from future
21 breaches.

22 75. To his knowledge, Plaintiff has not been the victim of any other data breach.

23 ***Securing Personal Information and Preventing Breaches***
24
25
26

1 76. Data breaches are preventable.¹⁶ As Lucy Thompson wrote in the DATA BREACH
 2 AND ENCRYPTION HANDBOOK, “In almost all cases, the data breaches that occurred could have
 3 been prevented by proper planning and the correct design and implementation of appropriate
 4 security solutions.”¹⁷ She added that “[o]rganizations that collect, use, store, and share sensitive
 5 personal data must accept responsibility for protecting the information and ensuring that it is not
 6 compromised”¹⁸

7
 8 77. “Most of the reported data breaches are a result of lax security and the failure to
 9 create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information
 10 security controls, including encryption, must be implemented and enforced in a rigorous and
 11 disciplined manner so that a *data breach never occurs*.”¹⁹

12 78. In a Data Breach like this, many failures laid the groundwork for the Breach. The
 13 FTC has published guidelines that establish reasonable data security practices for businesses. The
 14 FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks
 15 to computer systems, and implementing safeguards to control such risks.²⁰ The guidelines
 16 establish that businesses should protect the confidential information that they keep; properly
 17 dispose of personal information that is no longer needed; encrypt information stored on computer
 18 networks; understand their network’s vulnerabilities; and implement policies for installing vendor-
 19 approved patches to correct security problems. The guidelines also recommended that businesses
 20 utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming
 21
 22

23
 24 ¹⁶ Lucy L. Thomson, “Despite the Alarming Trends, Data Breaches Are Preventable,” in DATA BREACH AND
 ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

25 ¹⁷*Id.* at 17.

¹⁸*Id.* at 28.

26 ¹⁹*Id.*

²⁰ FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

1 traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted
 2 from the system; and have a response plan ready in the event of a breach.

3 79. Upon information and belief, Defendant failed to ensure that the MOVEit system
 4 maintained reasonable and necessary industry standards necessary to prevent a data breach,
 5 including the FTC's guidelines. Upon information and belief, Defendant also failed to ensure that
 6 the MOVEit system met the minimum standards of any of the following frameworks: the NIST
 7 Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk
 8 and Authorization Management Program (FEDRAMP); or the Center for Internet Security's
 9 Critical Security Controls (CIS CSC), which are well respected authorities in reasonable
 10 cybersecurity preparation.
 11

12 80. As explained by the Federal Bureau of Investigation, "[p]revention is the most
 13 effective defense against ransomware and it is critical to take precautions for protection."²¹
 14

15 81. To prevent and detect ransomware attacks, including the ransomware attack that
 16 resulted in the Data Breach, Defendant could and should have implemented, or ensured its vendors
 17 implemented, as recommended by the United States Government, the following measures:

- 18 • Implement an awareness and training program. Because end users are targets,
 19 employees and individuals should be aware of the threat of ransomware and
 20 how it is delivered.
- 21 • Enable strong spam filters to prevent phishing emails from reaching the end
 22 users and authenticate inbound email using technologies like Sender Policy
 23 Framework (SPF), Domain Message Authentication Reporting and
 24 Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent
 25 email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable
 26 files from reaching end users.

²¹ See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited July 17, 2023).

- 1 • Configure firewalls to block access to known malicious IP addresses.
- 2 • Patch operating systems, software, and firmware on devices. Consider using a
- 3 centralized patch management system.
- 4 • Set anti-virus and anti-malware programs to conduct regular scans
- 5 automatically.
- 6 • Manage the use of privileged accounts based on the principle of least privilege:
- 7 no users should be assigned administrative access unless absolutely needed; and
- 8 those with a need for administrator accounts should only use them when
- 9 necessary.
- 10 • Configure access controls—including file, directory, and network share
- 11 permissions—with least privilege in mind. If a user only needs to read specific
- 12 files, the user should not have write access to those files, directories, or shares.
- 13 • Disable macro scripts from office files transmitted via email. Consider using
- 14 Office Viewer software to open Microsoft Office files transmitted via email
- 15 instead of full office suite applications.
- 16 • Implement Software Restriction Policies (SRP) or other controls to prevent
- 17 programs from executing from common ransomware locations, such as
- 18 temporary folders supporting popular Internet browsers or
- 19 compression/decompression programs, including the AppData/LocalAppData
- 20 folder.
- 21 • Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- 22 • Use application whitelisting, which only allows systems to execute programs
- 23 known and permitted by security policy.
- 24 • Execute operating system environments or specific programs in a virtualized
- 25 environment.
- 26 • Categorize data based on organizational value and implement physical and
- logical separation of networks and data for different organizational units.²²

82. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, or ensured its vendors

²² *Id.* at 3-4.

implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks. . . .
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net). . . .
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it. . . .
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .²³

²³ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* <https://www.cisa.gov/news-events/news/protecting-against-ransomware> (last visited July 17, 2023).

83. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, or ensured its vendors implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; Remove privilege credentials

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- Apply principle of least-privilege

Monitor for adversarial activities

- Hunt for brute force attempts
- Monitor for cleanup of Event logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].²⁴

84. To prevent zero-day attacks, Defendant could and should have implemented, or ensured its vendors implemented, as recommended by Security Intelligence, the following:

²⁴ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited July 17, 2023).

- 1 • **Patch management:** Formal patch management can help security teams remain aware of critical patches.
- 2 • **Vulnerability management:** Vulnerability assessments and penetration tests can help companies detect zero-day vulnerabilities before adversaries find them.
- 3 • **Attack surface management (ASM):** ASM enables security teams to identify all network assets and scan them for vulnerabilities. ASM tools assess the network from an attacker's perspective, focusing on how threat actors might try to exploit assets.
- 4 • **Threat intelligence:** Security researchers are often the first to identify zero-day vulnerabilities. Organizations that receive threat intelligence updates may be informed about zero-day vulnerabilities sooner.
- 5 • **Anomaly-based detection methods:** Machine learning tools can spot suspicious activity in real-time. Common anomaly-based detection solutions include user and entity behavior analytics (UEBA), extended detection and response (XDR) platforms, endpoint detection and response (EDR) tools and some intrusion detection and intrusion prevention systems.²⁵

12 85. Defendant acquired, collected, and stored the PII of Plaintiff and Class Members.

13 86. Plaintiff and other Members of the Class entrusted their PII to Defendant.

14 87. By obtaining, collecting, and storing the PII of Plaintiff and Class Members,
15 Defendant assumed legal and equitable duties and knew or should have known that it was
16 responsible for protecting the PII from disclosure.

17 88. Plaintiff and Class Members have taken reasonable steps to maintain the
18 confidentiality of their PII and relied on Defendant to keep their PII confidential and securely
19 maintained, to use this information for business purposes only, and to make only authorized
20 disclosures of this information.

21 89. Given that Defendant was storing the PII of other individuals, Defendant could and
22 should have implemented all of the above measures, and ensured that its vendors did the same, to
23 prevent and detect ransomware attacks.
24

25
26

²⁵ <https://securityintelligence.com/news/the-moveit-breach-impact-and-fallout-how-can-you-respond/>.

1 90. The occurrence of the Data Breach indicates that Defendant failed to adequately
2 implement one or more of the above measures to prevent ransomware attacks, resulting in the Data
3 Breach and the exposure of the PII of Plaintiff and Class Members.

4 91. Defendant could have prevented this Data Breach by properly securing and
5 encrypting the folders, files, and or data fields containing the PII of Plaintiff and Class Members,
6 and ensuring the MOVEit software properly secured and encrypted the folders, files, and/or data
7 fields containing the PII of Plaintiff and Class Members. Alternatively, Defendant could have
8 destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-
9 accessible environment when there was a reasonable need to do so.

10 92. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is
11 exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data
12 as well as the direct warning from PSC of the vulnerability and likely exploitation of the
13 vulnerability.

14 93. Despite the prevalence of public announcements of data breach and data security
15 compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class
16 Members from being compromised.

17 94. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class
18 Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers,
19 fraudulent use of that information and damage to victims may continue for years.

20
21
22 ***The Value of PII***

23 95. The PII of individuals remains of high value to criminals, as evidenced by the prices
24 they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity
25 credentials. For example, personal information can be sold at a price ranging from \$40 to \$200,
26

and bank details have a price range of \$50 to \$200.²⁶ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.²⁷ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²⁸

96. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change.

97. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”²⁹

98. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

99. One such example of criminals using PII for profit is the development of “Fullz” packages.

100. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of

²⁶ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed July 17, 2023).

²⁷ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed July 17, 2023).

²⁸ *In the Dark*, VPNOOverview, 2019, available at: <https://vpnooverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed July 17, 2023).

²⁹ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed July 17, 2023).

1 accuracy in order to assemble complete dossiers on individuals. These dossiers are known as
2 “Fullz” packages.

3 101. The development of “Fullz” packages means that stolen PII from the Data Breach
4 can easily be used to link and identify it to Plaintiff’s and the Class’ phone numbers, email
5 addresses, and other unregulated sources and identifiers. In other words, even if certain
6 information such as emails, phone numbers, or credit card numbers may not be included in the PII
7 stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and
8 sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam
9 telemarketers) over and over.

11 102. That is exactly what is happening to Plaintiff and members of the Class, and it is
12 reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff’s and the Class’s
13 stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

14 ***Plaintiff and the Class Face Significant Risk of Continued Identity Theft***

15 103. Plaintiff and members of the proposed Class have suffered injury from the misuse
16 of their PII that can be directly traced to Defendant.

17 104. Defendant negligently disclosed the PII of Plaintiff and the Class for criminals to
18 use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed
19 the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices
20 and tactics, including online account hacking, unauthorized use of financial accounts, and
21 fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the
22 stolen PII.
23

24 105. As a result of Defendant’s negligence and failure to prevent the Data Breach,
25 Plaintiff and the Class have suffered and will continue to suffer damages, including monetary
26

1 losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of
 2 suffering:

- 3 a. The loss of the opportunity to control how their PII is used;
- 4 b. The diminution in value of their PII;
- 5 c. The compromise and continuing publication of their PII;
- 6 d. Out-of-pocket costs associated with the prevention, detection, recovery, and
 7 remediation from identity theft or fraud;
- 8 e. Lost opportunity costs and lost wages associated with the time and effort
 9 expended addressing and attempting to mitigate the actual and future consequences
 10 of the Data Breach, including, but not limited to, efforts spend researching how to
 11 prevent, detect, contest, and recover form identity theft and fraud;
- 12 f. Delay in receipt of tax refund monies;
- 13 g. Unauthorized use of stolen PII; and
- 14 h. The continued risk to their PII, which remains in Defendant's possession
 15 and is subject to further breaches so long as Defendant fails to undertake the
 16 appropriate measures to protect the Personal Information in their possession.

17 106. The fraudulent activity resulting from the Data Breach may not come to light for
 18 years.

19 107. There may be a time lag between when harm occurs versus when it is discovered,
 20 and also between when PII is stolen and when it is used. According to the U.S. Government
 21 Accountability Office ("GAO"), which conducted a study regarding data breaches:
 22

23 [L]aw enforcement officials told us that in some cases, stolen data may
 24 be held for up to a year or more before being used to commit identity theft.
 25 Further, once stolen data have been sold or posted on the Web, fraudulent use of
 26 that information may continue for years. As a result, studies that attempt to

1 measure the harm resulting from data breaches cannot necessarily rule out all future
2 harm.³⁰

3 108. Defendant's negligence and failure to properly notify Plaintiff and members of the
4 Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the
5 earliest ability to take appropriate measures to protect their PII and take other necessary steps to
6 mitigate the harm caused by the Data Breach

7 109. Plaintiff and Class Members now face years of constant surveillance of their
8 financial and personal records, monitoring, and loss of rights. The Classes are incurring and will
9 continue to incur such damages in addition to any fraudulent use of their Personal Information.

10 110. Defendant was, or should have been, fully aware of the unique type and the
11 significant volume of data contained in Defendant's database and on Defendant's MOVEit server,
12 amounting to potentially thousands of individuals' detailed, personal information and, thus, the
13 significant number of individuals who would be harmed by the exposure of the unencrypted data.

14 111. At all relevant times, Defendant knew, or reasonably should have known, of the
15 importance of safeguarding the PII of Plaintiff and Class Members, including Social Security
16 numbers, and of the foreseeable consequences that would occur if Defendant's data security
17 system was breached, including, specifically, the significant costs that would be imposed on
18 Plaintiff and Class Members as a result of a breach.

19 112. To date, Defendant has offered Plaintiff and some Class Members twenty-four (24)
20 months of identity monitoring services. The offered services are inadequate to protect Plaintiff and
21 Class Members from the threats they face for years to come, particularly in light of the Personal
22 Information at issue here.

23
24
25
26

³⁰ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed July 17, 2023).

113. The injuries to Plaintiff and Class Members are directly and proximately caused by Defendant's negligence and failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Defendant Failed to Adhere to FTC Guidelines

114. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

115. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."³¹ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."³²

116. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

- a. Protect the sensitive consumer information that they keep;
- b. Properly dispose of PII that is no longer needed;
- c. Encrypt information stored on computer networks;

³¹ 17 C.F.R. § 248.201 (2013).

³² *Id.*

1 d. Understand their network's vulnerabilities; and

2 e. Implement policies to correct security problems.

3 117. The guidelines also recommend that businesses watch for large amounts of data
4 being transmitted from the system and have a response plan ready in the event of a breach.

5 118. The FTC recommends that companies not maintain information longer than is
6 needed for authorization of a transaction; limit access to sensitive data; require complex passwords
7 to be used on networks; use industry-tested methods for security; monitor for suspicious activity
8 on the network; and verify that third-party service providers have implemented reasonable security
9 measures.
10

11 119. The FTC has brought enforcement actions against businesses for failing to
12 adequately and reasonably protect consumer data, treating the failure to employ reasonable and
13 appropriate measures to protect against unauthorized access to confidential consumer data as an
14 unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"),
15 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must
16 take to meet their data security obligations.
17

18 120. Defendant's negligence and failure to employ reasonable and appropriate measures
19 to protect against unauthorized access to Plaintiff and the Class's PII constitutes an unfair act or
20 practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

21 IV. CLASS ACTION ALLEGATIONS

22 121. Plaintiff brings this nationwide class action on behalf of herself and on behalf of
23 others similarly situated pursuant to Fed. R. Civ. P. 23 (b)(2), (b)(3), and (c)(4).
24

25 122. The Class that Plaintiff seeks to represent is defined as follows:

26 **All individuals whose PII may have been accessed and/or
acquired in the Data Breach that is the subject of the Notice of**

Data Breach that Defendant sent to Plaintiff and the Class Members on or around August of 2023.

123. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. According to the Attorney General for the State of Maine Data Breach Notifications, the total number of persons affected by the Data Breach is 429,252.

124. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. All had their PII compromised as a result of the Data Breach.

125. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their counsel.

126. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

1 **127. Commonality and Predominance:** There are many questions of law and fact
 2 common to the claims of Plaintiff and the other members of the Class, and those questions
 3 predominate over any questions that may affect individual members of the Class. Common
 4 questions for the Class include:

- 5 a. When Defendant actually learned of the Data Breach and whether its response was
 6 adequate;
- 7 b. Whether Defendant failed to adequately safeguard Plaintiff's and Class Members'
 8 PII;
- 9 c. Whether Defendant owed a duty to Plaintiff and the Class to ensure MOVEit was
 10 capable of adequately protecting their PII, and whether it breached this duty;
- 11 d. Whether Defendant breached its duties to Plaintiff and the Class as a result of the
 12 Data Breach;
- 13 e. Whether Defendant failed to ensure MOVEit provided adequate cyber security;
- 14 f. Whether Defendant knew or should have known that its computer and network
 15 security systems were vulnerable to cyber-attacks;
- 16 g. Whether Defendant's conduct, including its failure to act, resulted in or was the
 17 proximate cause of the breach of its company network;
- 18 h. Whether Defendant was negligent in utilizing MOVEit which permitted
 19 unencrypted PII of vast numbers of individuals to be stored within its network;
- 20 i. Whether Defendant was negligent in failing to ensure it adhered to reasonable
 21 retention policies, thereby greatly increasing the size of the Data Breach;
- 22 j. Whether Defendant breached implied contractual duties to Plaintiff and Class
 23 Members to use reasonable care in protecting their PII;
- 24
- 25
- 26

- 1 k. Whether Defendant failed to adequately respond to the Data Breach, including
2 failing to investigate it diligently and notify affected individuals in the most
3 expedient time possible and without unreasonable delay, and whether this caused
4 damages to Plaintiff and Class Members;
- 5 l. Whether Defendant continues to breach duties to Plaintiff and Class Members;
- 6 m. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant's
7 negligent actions or failures to act;
- 8 n. Whether Plaintiff and the Class are entitled to recover damages, equitable relief,
9 and other relief; and
- 10 o. Whether Defendant's actions alleged herein constitute gross negligence, and
11 whether Plaintiff and Class Members are entitled to punitive damages.
12

13 **V. CAUSES OF ACTION**

14 **FIRST CAUSE OF ACTION**
15 **NEGLIGENCE**
16 **(On Behalf of Plaintiff and the Class)**

17 128. Plaintiff incorporates by reference all preceding factual allegations as though fully
18 alleged here.

19 129. While providing its services, Defendant gathered and stored the PII of Plaintiff and
20 Class Members.

21 130. Defendant had full knowledge of the sensitivity of the PII and the types of harm
22 that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.
23 Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding,
24 safeguarding, and protecting that information. Plaintiff and Class Members were the foreseeable
25 victims of any inadequate safety and security practices. Plaintiff and the Class Members had no
26

1 ability to protect their PII that was in Defendant's possession. As such, a special relationship
2 existed between the Defendant and the Plaintiff and Class Members.

3 131. Defendant was well aware of the fact that cyber criminals routinely target
4 corporations through cyberattacks in an attempt to steal the PII of employees, applicants, business
5 associates, customers, and patients.

6 132. Defendant owed Plaintiff and Class Members a common law duty to use reasonable
7 care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing,
8 using, and managing personal information, including taking action to reasonably safeguard such
9 data and provide notification to Plaintiff and Class Members of any breach in a timely manner so
10 that appropriate action could be taken to minimize losses.

11 133. Defendant had duties to protect and safeguard the PII of Plaintiff and Class
12 Members from potential cyberattacks, including by ensuring MOVEit: (i) encrypted any document
13 or report containing PII, (ii) did not permit documents containing unencrypted PII to be maintained
14 on its systems, and (iii) took other similarly common-sense precautions when dealing with
15 sensitive PII. Additional duties that Defendant owed Plaintiff and Class Members include ensuring
16 it and its vendors:
17

- 18 a. Exercised reasonable care in obtaining, retaining, securing, safeguarding, deleting
19 and protecting the PII in its possession;
- 20 b. Protected the PII in its possession using reasonable and adequate security
21 procedures and systems;
- 22 c. Adequately and properly audited and tested its systems;
- 23 d. Adequately and properly audited, tested, and trained its employees regarding how
24 to properly and securely transmit and store PII;
- 25
- 26

- e. Trained its employees not to store PII for longer than absolutely necessary;
- f. Implement processes to quickly detect a data breach, security incident, or intrusion;
- and
- g. Promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

134. Plaintiff and Class Members were the intended beneficiaries of Defendant's duties, creating a special relationship between them. Defendant was in a position to ensure that MOVEit systems were sufficient to protect the PII that Plaintiff and the Class had entrusted to it Defendant.

135. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' PII. Defendant breached its duties by, among other things:

- a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;
- b. Failing to ensure MOVEit was capable of protecting the PII in its possession using reasonable and adequate security procedures and systems;
- c. Failing to ensure its and its vendors were adequately and properly auditing and testing its computer systems to avoid cyberattacks;
- d. Failing to ensure it and its vendors adequately and properly audited, tested, and trained its employees regarding how to properly and securely transmit and store PII, including maintaining PII in an encrypted format;
- e. Failing to ensure it and its vendors adequately and properly trained its employees not to store PII for longer than absolutely necessary;
- f. Failing to ensure it and its vendors consistently enforced security policies aimed at protecting Plaintiff and Class Members' PII;

- 1 g. Failing to implement processes to quickly detect data breaches, security incidents,
2 or intrusions;
- 3 h. Failing to ensure it and its vendors abided by reasonable retention and destruction
4 policies for PII of former employees, applicants, business associates, customers,
5 and patients; and
- 6 i. Failing to promptly and accurately notify Plaintiff and Class Members of the Data
7 Breach that affected their PII.

8
9 136. Defendant's willful failure to abide by these duties was wrongful, reckless, and
10 grossly negligent in light of the foreseeable risks and known threats.

11 137. As a proximate and foreseeable result of Defendant's grossly negligent conduct,
12 Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms
13 and damages (as alleged above).

14 138. The damages Plaintiff and Class Members have suffered (as alleged above) were
15 and are reasonably foreseeable.

16 139. The damages Plaintiff and the Class have and will suffer were and are the direct
17 and proximate result of Defendant's grossly negligent conduct.

18 140. Plaintiff and the Class have suffered injury and are entitled to actual and punitive
19 damages in an amount to be proven at trial.

20
21 **SECOND CAUSE OF ACTION**
22 **NEGLIGENCE *PER SE***
23 **(On Behalf of Plaintiff and the Class)**

24 141. Plaintiff incorporates by reference all allegations of the preceding paragraphs as
25 though fully set forth herein.

26 142. In addition to its duties under common law, Defendant had additional duties
imposed by statute and regulations, including the duties the FTC Act. The harms which occurred

1 as a result of Defendant's failure to observe these duties, including the loss of privacy and
2 significant risk of identity theft, are the types of harm that these statutes and their regulations were
3 intended to prevent.

4 143. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and
5 adequate computer systems and data security practices to safeguard Plaintiff and Class Members'
6 PII.

7 144. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce,"
8 including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as
9 Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders
10 also form part of the basis of Defendant's duty in this regard.

11 145. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures
12 to protect consumers PII and not complying with applicable industry standards, as described in
13 detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of
14 PII it obtained and stored, and the foreseeable consequences of a data breach including,
15 specifically, the damages that would result to Plaintiff and Class Members.

16 146. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se* as
17 Defendant's violation of the FTC Act establishes the duty and breach elements of negligence.

18 147. Plaintiff and Class Members are within the class of persons that the FTC Act was
19 intended to protect.

20 148. The harm that occurred as a result of the Data Breach is the type of harm the FTC
21 Act was intended to guard against. The FTC has pursued enforcement actions against businesses,
22 which, as a result of their failure to employ reasonable data security measures and avoid unfair and
23 deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.
24
25
26

1 149. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff
2 and Class Members, Plaintiff and Class Members would not have been injured.

3 150. The injury and harm suffered by Plaintiff and Class Members was the reasonably
4 foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that
5 it was failing to meet their duties, and that Defendant's breach would cause Plaintiff and Class
6 Members to experience the foreseeable harms associated with the exposure of their PII.

7
8 151. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and
9 Class Members have suffered injury and are entitled to compensatory, consequential, and punitive
10 damages in an amount to be proven at trial.

11 **THIRD CAUSE OF ACTION**
12 **BREACH OF IMPLIED CONTRACT**
13 **(On Behalf of Plaintiff and the Class)**

14 152. Plaintiff incorporates by reference all preceding factual allegations as though fully
15 alleged here.

16 153. Plaintiff's and Class Members' PII was provided to Defendant as a condition of
17 their receipt of its services.

18 154. When Plaintiff and Class Members provided their PII to Defendant as part of their
19 receipt of services, they entered into implied contracts in which Defendant agreed to comply with
20 its statutory and common law duties to protect their PII and to timely notify them in the event of a
21 Data Breach.

22 155. Based on Defendant's legal obligations and acceptance of Plaintiff's and Class
23 Members' PII, Defendant had an implied duty to safeguard their PII through the use of reasonable
24 industry standards.

25 156. Defendant breached the implied contracts by failing to safeguard Plaintiff's and
26 Class Members' PII and failing to provide them with timely and accurate notice of the Data Breach.

1 Indeed, it took Defendant approximately over two (2) months to begin warning Plaintiff and Class
2 Members of their imminent risk of identity theft.

3 157. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff
4 and the Class Members have suffered damages, including foreseeable consequential damages that
5 Defendant knew about when it requested Plaintiff's and the Class Members' PII.
6

7 158. Plaintiff and the Class have suffered injury, and are entitled to actual and punitive
8 damages, statutory damages, and reasonable attorneys' fees and costs, in an amount to be proven
9 at trial.

10 **FOURTH CAUSE OF ACTION**
11 **BREACH OF FIDUCIARY DUTY**
12 **(On Behalf of Plaintiff and the Class)**

13 159. Plaintiff incorporates by reference all preceding factual allegations as though fully
14 alleged here.

15 160. A relationship existed between Plaintiff and the Class Members and Defendant in
16 which Plaintiff and the Class put their trust in Defendant to protect their PII. Defendant accepted
17 this duty and obligation when it received Plaintiff and the Class Members' PII.

18 161. Plaintiff and the Class Members entrusted their PII to Defendant on the premise and
19 with the understanding that Defendant would safeguard their information, use their PII for business
20 purposes only, and refrain from disclosing their PII to unauthorized third parties.

21 162. Defendant knew or should have known that the failure to exercise due care in the
22 collecting, storing, and using of individual's PII, including ensuring that its vendors used such
23 care, involved an unreasonable risk of harm to Plaintiff and the Class, including harm that
24 foreseeably could occur through the criminal actions of a third party.
25

26 163. Defendant's fiduciary duty required it to exercise reasonable care in safeguarding,
securing, and protecting such information from being compromised, lost, stolen, misused, and/or

1 disclosed to unauthorized parties. This duty includes, among other things, ensuring and monitoring
2 its vendors' designing, maintaining, and testing of its security protocols to ensure that Plaintiff and
3 the Class's information was adequately secured and protected.

4 164. Defendant also had a fiduciary duty to ensure that its vendors had procedures in
5 place to detect and prevent improper access and misuse of Plaintiff's and the Class's PII.
6 Defendant's duty to use reasonable security measures arose as a result of the special relationship
7 that existed between Defendant and Plaintiff and the Class. That special relationship arose because
8 Defendant was entrusted with Plaintiff and the Class's PII.
9

10 165. Defendant breached its fiduciary duty that it owed Plaintiff and the Class by failing
11 to act in good faith, fairness, and honesty; by failing to act with the highest and finest loyalty; and
12 by failing to protect the PII of Plaintiff and the Class Members.

13 166. Defendant's breach of fiduciary duties was a legal cause of damages to Plaintiff and
14 the Class.

15 167. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and the Class
16 would not have occurred, and the Data Breach contributed substantially to producing the damage
17 to Plaintiff and the Class.
18

19 168. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff
20 and the Class are entitled to actual, consequential, and nominal damages and injunctive relief, with
21 amounts to be determined at trial.
22

23 **FIFTH CAUSE OF ACTION**
24 **BREACH OF IMPLIED CONTRACT**
(On Behalf of Plaintiff and the Class)

25 169. Plaintiff incorporates by reference all preceding factual allegations as though fully
26 alleged here.

1 170. When Plaintiff and Class Members provided their Personal Information to
2 Defendant as a condition of receiving services, Plaintiff and proposed class members entered into
3 implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect
4 such information and to timely and accurately notify Plaintiff and proposed class members that
5 their data had been breached and compromised.

6 171. Defendant solicited and invited Plaintiff and Class Members to provide their
7 Personal Information as a condition of receiving services from Defendant.

8 172. Plaintiff and Class Members accepted Defendant's offer and provided their PII
9 Defendant required, expecting that Defendant would exercise reasonable care to safeguard and
10 maintain the confidentiality of their PII.

11 173. Each disclosure of PII was made pursuant to the mutually agreed upon implied
12 contract with Defendant under which Defendant agreed to safeguard and protect such information
13 and to timely and accurately notify them that such information was compromised and breached.

14 174. Plaintiff and Class Members would not have provided and entrusted their PII in the
15 absence of such implied contract between them and the Defendant.

16 175. Plaintiff and Class Members fully performed their obligations under the implied
17 contracts with Defendant.

18 176. Defendant breached their implied contracts it made with Plaintiff and Class
19 Members by failing to safeguard and protect Plaintiff's and Class Members' PII through the
20 conduct detailed herein and by failing to provide timely and accurate notice to them that their PII
21 was compromised as a result of the Data Breach.

22 177. The losses and damages sustained by Plaintiff and Class Members as described
23 herein were the direct and proximate result of Defendant's breaches of the implied contracts
24

1 between it and the Plaintiff and Class Members.

2 **SIXTH CAUSE OF ACTION**
3 **INVASION OF PRIVACY**
4 **(On Behalf of Plaintiff and the Class)**

5 178. Plaintiff incorporates by reference all preceding factual allegations as though fully
6 alleged here.

7 179. Plaintiff and Class Members have a reasonable expectation of privacy in their PII.

8 180. Defendant's negligent, reckless, and intentional conduct as alleged herein invaded
9 Plaintiff's and Class Members' privacy.

10 181. By knowingly failing to keep Plaintiff's and Class Members' PII safe, and by
11 knowingly misusing and/or disclosing said information to unauthorized parties for unauthorized
12 use, Defendant negligently, recklessly, and intentionally invaded Plaintiff's and Class Members'
13 privacy by intruding into Plaintiff's and Class Members' private affairs, without approval, in a
14 manner that identifies Plaintiff and Class Members and that would be highly offensive and
15 objectionable to a person of ordinary sensibilities.

16 182. Defendant knew that an ordinary person in Plaintiff's or a Class Member's position
17 would consider Defendant's negligent, reckless, and intentional actions highly offensive and
18 objectionable.

19 183. Such an intrusion into Plaintiff's and Class Members' private affairs is likely to
20 cause outrage, shame, and mental suffering because the Personal Information disclosed contained
21 PII.

22 184. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded
23 into Plaintiff's and Class Members' private life by negligently, recklessly, and intentionally
24 misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear
25 consent.
26

1 185. The PII disclosed by Defendant has no legitimate reason to be known by the public.

2 186. Defendant intentionally concealed from Plaintiff and Class Members an incident
3 that misused and/or disclosed their Personal Information without their informed, voluntary,
4 affirmative, and clear consent.

5 187. As a proximate result of such intentional misuse and disclosures, Plaintiff's and
6 Class Members' reasonable expectations of privacy in their Personal Information was unduly
7 frustrated and thwarted. Defendant's conduct, amounting to a substantial and serious invasion of
8 Plaintiff's and Class Members' protected privacy interests causing anguish and suffering such that
9 a person with ordinary sensibilities would consider Defendant's intentional actions or inaction
10 highly offensive and objectionable.

11 188. In failing to protect Plaintiff's and Class Members' Personal Information, and in
12 negligently, recklessly, and intentionally misusing and/or disclosing their Personal Information,
13 Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's
14 and Class Members' rights to have such information kept confidential and private. Plaintiff,
15 therefore, seeks an award of damages on behalf of himself and the Class.

16
17
18 **SEVENTH CAUSE OF ACTION**
19 **BREACH OF COVENANT OF GOOD FAITH AND FAIR DEALING**
20 **(On Behalf of Plaintiff and the Class)**

21 189. Plaintiff incorporates by reference all preceding factual allegations as though fully
22 alleged here.

23 190. As described above, when Plaintiff and Class Members provided their PII to
24 Defendant, they entered into implied contracts in which Defendant agreed to comply with their
25 statutory and common law duties and industry standards to protect Plaintiff's and Class Members'
26 PII and timely detect and notify them in the event of a data breach.

1 191. These exchanges constituted an agreement between the parties: Plaintiff and Class
2 Members were required to provide their PII to Defendant in exchange for services provided by
3 Defendant.

4 192. It was clear by these exchanges that the parties intended to enter into an agreement.
5 Plaintiff and Class Members would not have voluntarily disclosed their PII to Defendant but for
6 the prospect of Defendant's promise of providing services. Conversely, Defendant presumably
7 would not have received Plaintiff's and Class Members' PII if it did not intend to provide services
8 to Plaintiff and the Class Members.

9 193. Implied in these exchanges was a promise by Defendant to ensure the Plaintiff's
10 and Class Members' PII was only used to provide services from Defendant.

11 194. Plaintiff and Class Members therefore did not receive the benefit of the bargain
12 with Defendant, because they provided their PII in exchange for Defendant's implied agreement
13 to keep it safe and secure.

14 195. While Defendant had discretion in the specifics of how they met the applicable laws
15 and industry standards, this discretion was governed by an implied covenant of good faith and
16 fair dealing.

17 196. Defendant breached this implied covenant when they engaged in acts and/or
18 omissions that are declared unfair trade practices by the FTC. These acts and omissions included:
19 failing to protect Plaintiff's and Class members' PII, failing to ensure its vendors possessed
20 adequate cybersecurity protection, and failing to timely notify and/or warn Plaintiff and Class
21 Members of the Data Breach.

22 197. Plaintiff and Class Members did all or substantially all the significant things that
23 the contract required them to do. All conditions required for Defendant's performance were met.
24

1 198. Defendant's acts or omissions unfairly interfered with Plaintiff's and Class
2 Members' rights to receive the full benefit of their contracts.

3 199. Plaintiff and Class Members have been or will be harmed by Defendant's breach
4 of this implied covenant in the many ways described above, including actual identity theft and/or
5 imminent risk of certainly impending and devastating identity theft that exists now that cyber
6 criminals have obtained their PII, and the attendant long-term expense of attempting to mitigate
7 and insure against these risks.
8

9 200. Defendant is liable for their breaches of these implied covenants, whether or not
10 they are found to have breached any specific express contractual term.

11 201. Plaintiff and Class Members are entitled to damages, including compensatory
12 damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.
13

14 **EIGHTH CAUSE OF ACTION**
15 **UNJUST ENRICHMENT**
16 **(On Behalf of Plaintiff and the Class)**

17 202. Plaintiff incorporates by reference all preceding factual allegations as though fully
18 alleged here.

19 203. Plaintiff and Class Members conferred a monetary benefit on Defendant by
20 providing Defendant with their valuable Personal Information.

21 204. Defendant enriched itself by saving the costs it reasonably should have expended
22 on data security measures to secure Plaintiff's and Class Members' Personal Information.

23 205. Instead of providing a reasonable level of security that would have prevented the
24 Data Breach, Defendant instead calculated to avoid their data security obligations at the expense
25 of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and
26 Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure
to provide the requisite security.

1 206. Under the principles of equity and good conscience, Defendant should not be
2 permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed
3 to implement appropriate data management and security measures that are mandated by industry
4 standards.

5 207. Defendant acquired the monetary benefit and Personal Information through
6 inequitable means in that it failed to disclose the inadequate security practices previously alleged.

7 208. If Plaintiff and Class Members knew that Defendant had not secured their Personal
8 Information, they would not have agreed to provide their PII to Defendant.

9 209. As a direct and proximate result of Defendant's conduct, Plaintiff and Class
10 Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft;
11 (ii) the loss of the opportunity how their Personal Information is used; (iii) the compromise,
12 publication, and/or theft of their Personal Information; (iv) out-of-pocket expenses associated with
13 the prevention, detection, and recovery from identity theft, and/or unauthorized use of their
14 Personal Information; (v) lost opportunity costs associated with effort expended and the loss of
15 productivity addressing and attempting to mitigate the actual and future consequences of the Data
16 Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and
17 recover from identity theft; (vi) the continued risk to their Personal Information, which remain in
18 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant
19 fails to undertake appropriate and adequate measures to protect Personal Information in their
20 continued possession; and (vii) future costs in terms of time, effort, and money that will be
21 expended to prevent, detect, contest, and repair the impact of the Personal Information
22 compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class
23 Members.
24
25
26

1 210. As a direct and proximate result of Defendant's conduct, Plaintiff and Class
2 Members have suffered and will continue to suffer other forms of injury and/or harm.

3 211. Defendant should be compelled to disgorge into a common fund or constructive
4 trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from
5 them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and
6 Class Members overpaid for Defendant's services.

7
8 **NINTH CAUSE OF ACTION**
9 **Injunctive and Declaratory Relief**
 (On Behalf of Plaintiff and the Class)

10 212. Plaintiff incorporates by reference all preceding factual allegations as though fully
11 alleged here.

12 213. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C.
13 § 2201.

14 214. As previously alleged and pleaded, Defendant owes duties of care to Plaintiff and
15 Class Members that require them to adequately secure their PII.

16 215. Defendant still possess the PII of Plaintiff and the Class Members and still stores it
17 on the MOVEit software.

18 216. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff
19 and the Class Members.

20 217. Defendant has claimed that it is taking some steps to increase its data security, but
21 there is nothing to prevent Defendant from reversing these changes once it has weathered the
22 increased public attention resulting from this Breach, and to once again place profits above
23 protection.

24 218. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security
25
26

1 measures do not comply with its contractual obligations and duties of care to provide adequate
2 security, and (2) that to comply with its contractual obligations and duties of care, Defendant must
3 implement and maintain reasonable security measures, including, but not limited to:

- 4 a. Ordering Defendant to ensure third-parties possessing its patients' PII engage
5 third-party security auditors/penetration testers as well as internal security
6 personnel to conduct testing, including simulated attacks, penetration tests, and
7 audits on its systems on a periodic basis, and ordering Defendant to promptly
8 correct any problems or issues detected by such third-party security auditors;
- 9 b. Ordering Defendant to significantly increase its spending on cybersecurity
10 including systems and personnel;
- 11 c. Ordering Defendant to engage third-party security auditors and internal
12 personnel to run automated security monitoring;
- 13 d. Ordering that Defendant guarantee third-parties possessing its patients' PII
14 audit, test, and train their security personnel regarding any new or modified
15 procedures;
- 16 e. Ordering that Defendant protect Plaintiff's and the Class's PII by, among other
17 things, guaranteeing third-parties possessing its patients' PII have firewalls and
18 access controls so that if one area of the third-parties' systems are compromised,
19 hackers cannot gain access to other portions of its systems;
- 20 f. Ordering that Defendant cease storing unencrypted PII on its systems;
- 21 g. Ordering that Defendant ensure that third-parties possessing its patients' PII
22 conduct regular database scanning and securing checks;
- 23 h. Ordering Defendant to ensure third-parties possession its patients' PII routinely
24
25
26

1 and continually conduct internal training and education to inform internal
 2 security personnel how to identify and contain a breach when it occurs and what
 3 to do in response to a breach;

- 4 i. Ordering Defendant to implement and enforce adequate retention policies for
 5 PII, including destroying, in a reasonably secure manner, PII once it is no longer
 6 necessary for it to be retained; and
 7
 8 j. Ordering Defendant to meaningfully educate its current, former, and
 9 prospective employees and subcontractors about the threats they face as a result
 10 of the loss of their financial and personal information to third parties, as well as
 11 the steps they must take to protect themselves.

12 **VI. PRAYER FOR RELIEF**

13 WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

- 14 a. An order certifying this action as a class action under Fed. R. Civ. P. 23,
 15 defining the Class as requested herein, appointing the undersigned as Class
 16 counsel, and finding that Plaintiff is a proper representative of the Class
 17 requested herein;
 18
 19 b. A judgment in favor of Plaintiff and the Class awarding them appropriate
 20 monetary relief, including compensatory damages, punitive damages,
 21 attorneys' fees, expenses, costs, and such other and further relief as is just and
 22 proper;
 23 c. An order providing injunctive and other equitable relief as necessary to protect
 24 the interests of the Class as requested herein;
 25 d. An order requiring Defendant to pay the costs involved in notifying the Class
 26 Members about the judgment and administering the claims process;

- 1 e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and
2 post-judgment interest, reasonable attorneys' fees, costs and expenses as
3 allowable by law; and
4 f. An award of such other and further relief as this Court may deem just and
5 proper.

6 **I. DEMAND FOR JURY TRIAL**

7 Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Class Action
8 Complaint.

9 Dated: September 1, 2023.

10 EMERY | REDDY, PLLC

11 /s/ Timothy W. Emery

12 /s/ Patrick B. Reddy

13 TIMOTHY W. EMERY

14 WSBA No. 34078

PATRICK B. REDDY

15 WSBA No. 34092

EMERY REDDY, PLLC

16 600 Stewart St., Ste 1100

Seattle, WA 98101

17 Telephone: (206) 442-9106

18 Fax: (206) 441-9711

Email: emeryt@emeryreddy.com

Email: reddyp@emeryreddy.com

19 William B. Federman*

20 **FEDERMAN & SHERWOOD**

21 10205 North Pennsylvania Avenue

Oklahoma City, Oklahoma 73120

22 Telephone: (405) 235-1560

23 Facsimile: (405) 239-2112

-and-

24 212 W. Spring Valley Road

Richardson, TX 75081

Email: wbf@federmanlaw.com

25 *pro hac vice request forthcoming

26 *Counsel for Plaintiff and Proposed Lead for
the Putative Class*

EXHIBIT 1



UMPQUA BANK

Consumer Banking Support
707 W Main Ave
Suite 450
Spokane, WA 99201

[REDACTED]
Roberto chapman
[REDACTED]

Re: Notice of Data Security Incident:

Dear Customer:

On Thursday June 22, we shared via email that personal information for a segment of Umpqua's customers was accessed due to a third-party vendor's exposure in the global MOVEit Transfer cybersecurity incident. **Our investigation has unfortunately revealed that your name and Social Security number were involved in this incident.** No banking information was involved, and you should continue to bank as you always do. We understand this news is frustrating and apologize for the inconvenience.

Your relationship with us is very important and safeguarding your personal and financial information is a responsibility we take seriously. We have been working closely with the involved vendor to provide 24 months of identity monitoring and theft resolution services to you at no charge. Additionally, you now have access to a toll-free dedicated call center to address questions related to the incident.

We have no evidence at this time that your personal information has been used in an unauthorized way, but we are sending this letter to:

- Communicate what happened.
- Identify the personal information involved.
- Provide details on how to enroll in 24 months of identity monitoring and theft resolution services we are offering to you at **no charge.**

What Happened

On May 31, 2023, Progress Software reported a previously unknown vulnerability in its MOVEit Transfer tool. Thousands of companies, including one of our third-party vendors, use this file transfer tool to move data files. This vendor provides technology services to many of the world's leading banks, including Umpqua. Upon notification, the vendor immediately suspended use of the MOVEit Transfer tool, and it remained disabled until they received and implemented a software patch to remediate the issue. Our vendor also launched an immediate investigation working alongside cyber experts and appropriate law enforcement agencies. On June 21, 2023, the vendor notified us that an unauthorized third party potentially accessed certain files transferred through MOVEit Transfer that contained some Umpqua Bank customer information. We then worked diligently to review the files, identify current contact information, and notify our potentially involved customers.

There is no evidence at this time that your personal information has been used in an unauthorized way.

What Information Was Involved

The personal information involved included your name and Social Security number.

What We Are Doing

Safeguarding your personal information is always our highest priority. Once Umpqua was notified of the MOVEit vulnerability, we took immediate action to confirm the security of our systems and implemented steps to further protect customer data, including launching an investigation into potential exposure among our third-party service providers.

When we learned about the potential involvement of Umpqua Bank customer information in the MOVEit Transfer incident, we immediately worked with our vendor to ensure that they had resolved the vulnerability to keep our customer information safe following the incident and moving forward. We can confirm that, upon learning of the incident, the vendor took steps to secure their environment and that they have further validated that security using a third-party forensics firm.

What You Can Do

To help protect your identity, we are offering a complimentary 24-month membership to OnAlert™ from ChexSystems®. OnAlert provides you with identity monitoring and can assist with the resolution of identity theft. **To activate your membership in OnAlert and start monitoring your personal information please enroll at [REDACTED] by December 31, 2023.** Your link will not work after this date. You will need to provide the website link noted above as proof of eligibility for this offer.

For new member questions and assistance with enrollment, please contact the OnAlert customer care team at (833) 919-4756. A credit card is **not** required for enrollment into OnAlert.

Once you enroll, you can contact OnAlert's customer care team **immediately** regarding any fraud issues. If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve it, an OnAlert agent will support you with investigation and resolution of each incident of potential fraud.

With OnAlert, you will have access to the following features:

- **Tri-Bureau Credit Report and Manual VantageScore® from Experian®, TransUnion®, and Equifax®:** Credit reports and scores from Experian, TransUnion, and Equifax.
- **Tri-Bureau Credit Monitoring from Experian, TransUnion, and Equifax:** Actively monitors credit bureau files and alerts you of key changes and indicators of fraud.
- **Automatic VantageScore Tracker:** Shows you your credit score so you can see how lenders evaluate your creditworthiness.
- **VantageScore Simulator:** Interactive credit score simulator you can use to see how actions will potentially impact your credit score.
- **Personalized Credit & Identity Alert Videos:** Credit and identity education videos.
- **Real Time Authorization Alerts:** Notifications of when your personal information is used for new applications or identity authorizations.
- **Dark Web Monitoring:** Internet and dark web surveillance monitoring of your personal information.
- **ChexSystems Monitoring and Alerts:** Actively monitors ChexSystems' database and alerts you of key activity and indicators of fraud. Chex Systems, Inc. (ChexSystems) is a nationwide specialty consumer reporting agency under the Fair Credit Reporting Act (FCRA).
- **Full-Service Restoration:** Certified Identity Theft Restoration Specialists available for assignment to help you address credit and non-credit related fraud.
- **Lost Wallet Assistance:** Protection of your personally identifiable information that has been compromised.
- **Up to \$1MM Identity Theft Insurance**:** Reimbursement for certain ancillary expenses associated with restoring your identity.

* Calculated on the VantageScore 3.0 model. Your VantageScore 3.0 from Experian® indicates your credit risk level and is not used by all lenders, so don't be surprised if your lender uses a score that's different from your VantageScore 3.0.

**The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Steps You Can Take

To help protect your personal information, we strongly recommend you do the following:

- Carefully review bank, credit card company, or other financial institutions as well as government institutions like the Internal Revenue Service (IRS) statements. Notify the statement sender immediately by phone and in writing if you detect any suspicious transactions or other activity you do not recognize.
- Enroll in OnAlert, the identity monitoring service that we are offering you. You will receive alerts about any effort to use your name and social security number to establish credit. The service will block that credit from being established if it is not you trying to initiate it.
- Additional steps and resources are available in the accompanying **Reference Guide**. We encourage you to read and follow these steps as well.

For More Information

Incident Information

For information about the MOVEit cybersecurity incident, please contact our vendor's dedicated call center.

1-833-919-4756

Monitoring Service Support

For support with setting up your OnAlert identity monitoring and threat resolution services, please contact the OnAlert call center.

1-833-919-4756

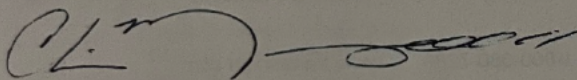
General Banking Information

For any other information related to your accounts or services, contact us.

1-866-486-7782

Please know that we take this matter very seriously, and we apologize for the concern and inconvenience this may cause you.

Sincerely,



Chris Merrywell
President, Consumer Banking
Umpqua Bank